INCIDENT RESPONSE SERVICES

Detect, prevent and respond to cyber threats at each stage of the attack lifecycle

The evolving nature of threat landscape means that even with strict security controls in place, your business is not immune to being compromised. Timely and efficient incident response helps to minimize the incurred losses, and in some cases, even prevent them along with recovering your IT infrastructure and business processes within the shortest time.

77% of companies

do not have a cyber security incident response plan in 2018

191 days

is the average length of time it takes for organizations to identify a data breach

Our Approach

We use real-life scenarios and understand how threat actors operate, leveraging this knowledge from our own incident response and investigation activities as well as Group-IB Threat Intelligence, recognized by top industry researchers.

Our Difference

Incident-centric approach

15 years of hands-on incident response experience within different verticals enable us to align our response tactics to a variety of threat models.

Certified experts

16,000 hours of incident response has been conducted by our forensic specialists who are internationally recognized members of advisory councils around the world

State-of-art- technologies

Empowering our world-class threat intelligence with advanced machine learning algorithms to offer a full range of incident response services.

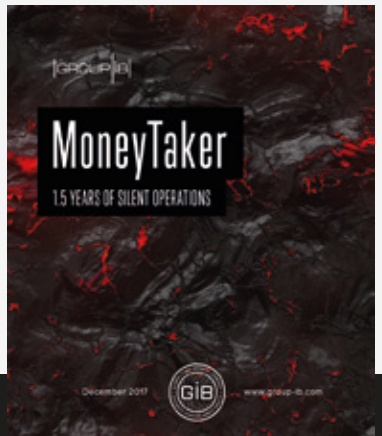
Group-IB's unique proprietary solutions enable rapid and efficient response to minimize impact and speed recovery.

Threat Intelligence

Actionable, finished intelligence to track actors and prevent attacks before they happen.

Threat Detection System

Intelligence-driven network protection even from the most advanced attacks.



Case from Group-IB's report:

One US bank was robbed twice due to incomplete incident response

About 20 companies were attacked in the US, UK and Russia by MoneyTaker group from May 2016 to November 2017. The average loss from each successful attack was about $500 000 baseline.

What you get:

Clear network infrastructure

We gather all necessary information for creating a list of Indicators of Compromise, write YARA-rules to clear your enterprise's network from the infiltration.

Investigative report with attacker profile

Our experts explore the anatomy of the attack — how attackers gained a foothold and moved laterally inside your organization to steal confidential data.

Remediation report and recommendations

After analysis we prepare a detailed report on how to adjust your security architecture and processes to strengthen your security posture.

Group-IB's Retainer

For your peace of mind, rely on our Retainer service to get an emergency assistance and avoid "a when seconds count" scenario.

Our Retainer Benefits:

- pre-negotiated terms and conditions to shorten response time
- discounted rates for additional prepaid support hours and IR services
- access to a 24/7 incident response hotline

We address the cyber kill chain at each phase

Our team of certified forensic experts has a clear understanding of your adversary's methodology to catch and stop threats at each phase of the kill chain.

Attack phase	Group-IB's defensive actions
Reconnaissance	TDS implementation for network traffic monitoring and suspicious behavior detection to unhide the attackers before they steal data.
Weaponization	Using Threat Intelligence reports to gather information about malicious programs or scripts and weaponized documents used by attackers.
Delivery	Applying TDS Polygon sandboxing technology for advanced threat detection and Threat Intelligence notifications for predicting upcoming phishing campaigns.
Exploitation	Threat Intelligence usage to analyze information about recently used exploits, patch your servers and workstations to deny access to your company's environment.
Installation	Using proprietary solutions to detect emerging of potentially malicious content and hunt for recently discovered threats.
Command & Control	TDS Sensor to detect C2 network connections, 24/7 log analysis is performed by experienced CERT specialists.
Actions on Targets	If localization of the incident was unsuccessful and attackers started lateral movement, our IR team comes to the facility for damage assessment and remediation.

Contact us to learn more about Incident Response Services

GROUP-IB

lab@group-ib.com
group-ib.com

London
+44 2036085907

New York
+1 202 774-95-91

Dubai
+971 8000 3570 4569